ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Survey on Privacy-Preserving and Authenticated Routing in Mistrustful Mobile Ad-Hoc Networks

Swetha M.S[1], Dr. Thungamani M [2], Pooja Reddy[3], Richa Singh [4]

Assistant Professor, Dept. of ISE, BMSIT & Management, Bangalore, India[1]

Assistant Professor, Dept. of CSE, COH UHS Campus GKVK, Bangalore, India[2]

Students 8 th Semester, Dept. of ISE, BMSIT & Management, Bangalore, India[3,4]

ABSTRACT: In most common mobile ad hoc networking scenarios, nodes establish communication based on long lasting public identities. However in some hostile and suspicious settings, node identities must not be exposed. Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. A number of anonymous routing schemes have been proposed for ad hoc networks in recent years, and they provide different level of secure protection at different cost. These schemes are more scalable to network size, but require more computation effort. Ad hoc routing protocols with the provisions for anonymity both protect the privacy of nodes and also restrict the collection of network information by malicious nodes. Until recently, quite a number of anonymous routing protocols have been proposed. Many of them, however, do not make allowance for authentication However, existing schemes provide only anonymity and non-availability, while non-observability is never considered or implemented by now. The main drawback in existing schemes is that packets are not secure as a whole. A secure privacy-preserving routing protocol APPRP that achieves content non-observability by employing anonymous key establishment based on group signature. APPRP is to protect all parts of a packet's content and it is independent of solutions on traffic pattern non-observability. The non- observable routing protocol is then executed in two phases. First, a secure key establishment process is performed to construct secret session keys. Then a non observable route discovery process is executed to find a route to the destination.

KEYWORDS*:* Mobile Communication, anonymity, group signature, ID-based encryption.

I. INTRODUCTION

The unique features of Mobile Ad Hoc Networks (MANET), such as open medium, dynamically changing topology, possible node compromise, difficulty in physical protection, lack of trust among nodes, and limited resources (processing power, storage power, bandwidth and energy), make MANET inherently vulnerable to various attacks. In wired networks, devices like desktops are always static and do not move from one place to another. Hence in wired networks there is no need to protect users' mobility behaviour or movement pattern, while this sensitive information should be kept private from adversaries in wireless environments. To achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern. Hence we further refine unobservability into two types one is content Unobservability, referring to no useful information can be extracted from content of any message and another one is Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic. With regard to privacy-related notions in communication networks, we follow the terminology on anonymity, unlinkability, and unobservability. These notions are defined with regard to item of interest (IOI, including senders, receivers, messages, etc.) as follows:

- Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.
- Unlinkability of two or more IOIs means these IOIs are no more or no less related from the attacker's view.
- Unobservability of an IOI is the state that whether it Exists or not is indistinguishable to all unrelated subjects, and subjects related to this IOI are anonymous to all other related subjects.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Privacy protection in routing of MANET has interested a lot of research efforts. A number of privacy-preserving routing schemes have been brought forward. However, existing anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET, most of them exploit asymmetric feature of public key cryptosystems to achieve their goals. Complete unlinkability and unobservability are not guaranteed due to incomplete content protection. Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc.

Entity Anonymity: The identity of the entity must not be revealed from forwarded packets in the network. In fact, it should not be possible for a participating node and an adversary to recognize the identity of a certain node from the transmitted packets.

Route Anonymity: For given routes even legitimate entity cannot map the node in a route and real identity of a source, an intermediate, and a destination node. This also implies that a source node, a destination node, and intermediate nodes can conduct route discovery without knowledge of any public route information.

Location/Topology Anonymity: Even if network traffic can be observed, network topology such as the number of nodes, link information, hop count must be veiled from adversary and participating nodes.Unfortunately, unlinkability alone is not enough in hostile environments like battlefields as important information like packet type is still available to attackers. Then a passive attacker can mount traffic analysis based on packet type far from an easy task because it is extremely difficult to hide information on packet type and node identity. Furthermore, a hint on using which key for decryption should be provided in each encrypted packet, which demands careful design to remove linkability. Another drawback of most previous schemes is that they rely heavily on public key cryptography, and thus incur a very high computation overhead. Among these requirements unobservability is the strongest one in that it implies not only anonymity but also unlinkability.

To achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern. Hence we further refine unobservability into five types: 1) Content Unobservability, referring to no useful information can be extracted from content of any message; 2) Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.3) Analysis of different anonymous routing schemes 4) Comparison of various routing protocols 5) Implemented USOR on ns2 and compared its performance with implementation of AODV.

The contributions of this paper include:

1) We provide a thorough analysis of existing anonymous routing schemes and demonstrate their vulnerabilities.

2) We propose APPRP, to our best knowledge, the first unobservable routing protocol for ad hoc networks, which achieves stronger privacy protection over network communications.

3) Detailed security analysis and comparison between APPRP and other related schemes are presented in the paper.

4) We implemented APPRP on ns2 and evaluated its performance by comparing it with the standard implementation of AODV in ns2. In next section, we discuss related work on anonymous routing schemes for ad hoc networks. After that we analyze the proposed scheme against various attacks. We also compare it with other anonymous routing schemes.

II. RELATED WORK

A number of privacy preserving schemes has been proposed in the recent years and they provide different level of privacy preservation at different cost. A. Based on one-time public/private key pairs

In 2003 Jiejun Kong and Xiaoyan Hon, proposed ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks. ANODR uses onion routing for route discovery and private/public key for obtaining anonymity. It offers sender, receiver, and route anonymity as well as sender and receiver unobservability. The route discovery method establishes an on-demand route between its source and destination. The disadvantages of ANODR are, 1) Each forwarding node has to generate a fresh public/secret key pair for each RREQ message it forwards. 2) For a node to decide whether it has to forward a RREP or not, it has to decrypt it with every private key. Each node encrypts the routing information with its own secret key during the route discovery so that the source and destination does not know the whole route.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

B. Public key cryptosystems

Denh Sy, Rex Chen and Lichun Bao proposed ODAR, an On-Demand Anonymous Routing protocol for wireless ad hoc networks. ODAR provides complete anonymity of nodes, links and source routing paths using bloom filters. The use of bloom filters is to provide ODAR storage, processing and communication efficiencies. ODAR provides only identity anonymity but not unlinkability, and RREQIRREP packets are not protected with session keys.

C. Based on public key cryptography and group signature

In 2011, Karim El Defrawy, and Gene Tsudik proposed ALARM, it makes use of public key cryptography and the group signature to preserve privacy. The group signature has good privacy preserving feature, in this everyone can verify a group signature but cannot identify who is the signer. But ALARM leaks a lot of sensitive privacy information such as network topology, location of every node, etc. By using this group signature ALARM construct one-time pseudonyms that are used to identify nodes at certain locations. This works with any group signature scheme and any location based protocol that can be used to route data between nodes. Even if a portion of the nodes are stationary, or if the speed of movement is not very high the node privacy is preserved.

D. Based on long-term public/private key pairs

Azzedine Boukerche, Khalil EI-Khatib,Larry Korba, Li Xu proposed a distributed routing protocol which guarantees security, anonymity and high reliability. SDAR use long-term public/private key pairs at each node for anonymous communication. SDAR introduces the notion of trust management system. The purpose of this system is to motivate the nodes to help each other and relaying data traffic. SDAR also identifies the malicious nodes, and avoids the nodes during the route establishment. The identification of malicious nodes makes it easy to take them out of the network, thereby increasing the route's security and reliability.

III. PROBLEMS OF EXISTING PROTOCOL

ANODR [10] which is based on onion routing is a anonymous protocol in that each intermediate node en- crypt forwarding packet by its public key and decrypt route reply packet by its private key. In route request, pack- ets are added an encrypted layer that is called boomerang onions. Most of the anonymous routing protocols have similar method with ANODR to find the destination. Cheng et al. Proposed ASRP based on public key encryption. The existing anonymous routing protocols , not only protocols mentioned above but most of anonymous routing protocols, are not concern with authentication. This means an adversary can illegitimately behave without any restrictions during the routing discovery. In particularly, these protocols are fragile against the DoS (denial of service) attack in that an ad hoc network is the broad- cast based wireless network. In more detail, if the exterior adversary who wants to inflict the overload on the network broadcasts route request packets or re-broadcasts existing control packets, the network resource would be shortly exhausted by maliciously propagated packets. Therefore, for blockading DoS attack, routing protocol must limit that adversary can broadcast packet in its disposition, and also re- played packets must be meaningless to prevent it roaming.

1. Group Signatures

In the group signature scheme, each group member can generate its own signature by its own private key issued from TA (trust authority). And also, each member can ver- ify signature without the signer's identity. Note that group signature scheme provides the authentication without dis- turbing the anonymity. If an anonymous routing protocol is properly combined with the group signature scheme, the routing protocol can retain the anonymity and authentica- tion at once. We use the terms of for group signature, classified the attribute of the group signature such like *anonymity*, *exculpability*, *traceability*, *framing*, *unlinkability*, *unforgeability*. Commonly, a group signature scheme is made up of three parts of key and four parts of function. Keys of group signature are group public key : *gpk*, group secret key :

gski, and group master key : *gmk*. *gpk*, *gski* , and *gmk* are made from EXTRACT by TA, as follow.

$$(gski\ ,\ gpk,\ gmk) \leftarrow \text{EXTRACT}(t) \qquad (1)$$

where k is a security parameter and i is the number of group members. Sign is a group signature algorithm using $gsk[i]$ and generate group signature σ by participating group member.

$$\sigma i \leftarrow \text{SIGN}gsk_i\,(m) \qquad (2)$$

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

where m is a message. Although each i-th member's group signature σ is different from each other, anyone cannot recognize the i-th identity from signature value. Only TA can trace the signer's identity. VERIFY is a verification algorithm using *gpk*.

$$\text{true } or \text{ false} \leftarrow \text{VERIFY}_{gpk}(m, \sigma i) \quad (3)$$

where true and false respectively mean verification success and verification failure. OPEN is used in tracing identity of signer only by TA and its master secret *gmk*. Member

$$i\text{'s identity} \leftarrow \text{OPEN}_{gmk}(m, \sigma i, gpk) \quad (4)$$

So far, numerous superb group signature schemes have been proposed in the literature. And also, they can be applied for our protocol if a scheme holds the properties as stated above.

2. Outsider Attacks

A passive outsider eavesdropping on all LAMs can, at most, obtain exactly the same information available to any legitimate MANET node (i.e., the current topology snap- shot). This would only happen if keys used to encrypt all communication in the MANET are leaked. Thus, a passive outsider is at most as powerful as a passive insider and, thus, protection against it is guaranteed as a side effect of thwarting passive insider attacks. Since group signatures attached to each LAM are untraceable and unlinkable, the only way to track nodes is by guessing possible trajectories. However, as discussed in Section 3, our MOBILITY assumption involves a minimum number of nodes (k out of n) moving within each time-slot. Thus, tracking movements of a given node translates into k-anonymity, i.e., the problem of identifying one out of k possible nodes. However, we note that, if LAM-s are encrypted using a group-wide key, topology information would become completely "invisible" to eavesdroppers.

3. **Passive Insider Attacks**

A passive insider (legitimate MANET node) can by design obtain all LAMs and determine their authenticity by verifying corresponding group signature. But also by design it can neither identify nor link nodes that generated these LAMs,since group signatures are untraceable. With other means of collecting mobility information eg: By visual monitoring, can determine that a certain node remain stationary. This might happen if in two consecutive time slots,the insider physically observes lack of mobility and also receives two LAMs referring to the same location.

ALARM Extension	Sybil Attack	Location-fraud Attack
Group Signatures with Self-Distinction	Prevent	Fail
One-Time Certificates	Prevent	Fail
Sequential Aggregate Signatures (SAS)	Prevent	Prevent
Secure Hardware	Prevent	Prevent

Table 1 Security Extensions against active Insider attacks

IV. APPRP: ANONYMOUS PRIVACY PRESERVING ROUTING PROTOCOL

In routing, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbours, then it can use such a key to encrypt the whole packet for a corresponding neighbour. The receiving neighbours can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pair wise key are needed. As a result, APPRP comprises two phases: anonymous trust establishment and unobservable route discovery.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A. Key Establishment Phase

Here, each and every node in the network communicates with its direct neighbours within its radio range for key establishment. The source node generates a random number and then computes a signature using its private signing key any one can verify this using group public key and after which broadcast to its neighbourhood. Once the neighbours receives it, it checks for the signature and if successful then the neighbourhood node computes the signature using its own signing key and computes the session key and reply to the source node. A pair wise key is constructed anonymously, as a result of which the messages exchanged are not observable.

B. Route Discovery Phase

Depending on the keys established on the previous phase, route discovery process is initiated. This phase consist of route request, route reply and data transmission. Route request (RREQ): Let the transmission between two nodes say, S and B. The node S chooses a random number and uses the identity of node B to encrypt the trapdoor information that can be opened only by private ID-based key of B. For route request process S chooses another random number which is considered as a route pseudonym and a sequence number. To ensure that unobservability is met, S chooses nonce which is updated. On receiving the RREQ message from S, the intermediate node tries to check out which one matches by trying out with all session keys shared by the neighbouring nodes. Fig.1 shows the Route Discovery of APPRP.Route Reply (RREP): Once the node B realizes it is the destination node, B starts to make the RREP message to the source node S. Broadcast technique is used for route reply messages. The node B chooses a random number and computes a cipher text to make aware that it is the valid destination capable of opening the information. Once route reply is carried out, before the data transmission, the node checks for load that is being transferred. In this case a intrusion detecting node is placed in between the other nodes. If the load is greater than the threshold, attack is detected and a secure data transmission is carried out. If the load is less than the maximum limit and if the new profile is less than the maximum threshold, then there is no attack.

C. Unobservable Data Transmission

Once the source node S finds out its successful destination to be B, it can start data transmission using pseudonyms and keys that is generated in earlier phases to achieve unobservability. On receiving the message from S, the intermediate node will know that the message is for them. After the decryption by the right key, it will know to whom the data packet must be sent next. Thus the data packet must be forwarded by the intermediate nodes until it reaches the destination node B.

V. SIMULATION RESULTS

The proposed routing scenario is implemented using NS2. The NS2 consist of two languages: C++ and Object- oriented Tool Command Language (OTCL). C++ defines the internal mechanisms of the simulation objects as well as scheduling discrete events. together using TclCL. Under the topology formation, 50 nodes are randomly distributed within a network field of 1680×970 meter such as a rectangle field. The traffic type is 512-byte CBR traffic. The node receives necessary cryptographic data to participate in the network. Each node stores a unique identity and public/private key pair with a certificate, the public key of the key server, and the required cryptographic data for the key exchange protocol. The IDS node checks for the load to detect attacks if any. The implementation result gives acceptable performance in terms of packet delivery ratio, packet delivery latency. But this protocol achieves anonymity, complete unlinkabilty, unobservability in terms of content and traffic and more over resists completely can achieve unobservability without too much computation cost. Table.1 shows the simulation parameters.

A. Topology Formation & Anonymous Key establishment

Constructing project design in NS2 should takes place. Fig.2 shows Topology Formation & Anonymous Key establishment.

B. Secure Privacy-Preserving Route Discovery

This phase is a privacy-preserving route discovery process based on the keys established in previous phase. Similar to normal route discovery process, our discovery process also comprises of route request and route reply. Under the protection of these session keys in the first phase, the route discovery process can be initiated by the source node to discover a route to the destination node. Fig.3 shows Secure

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

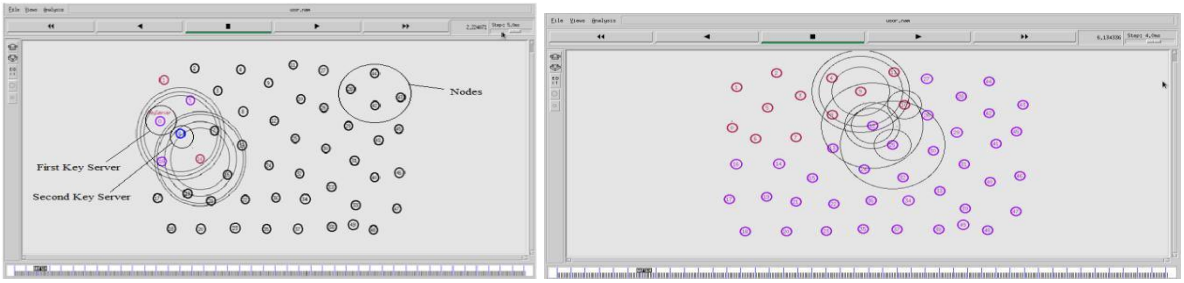

Fig.2 Topology Formation & Anonymous Key establishment and Secure Privacy-Preserving Route Discovery.

1) In APPRP only trusted neighbors will forward route packets for each other, otherwise packets are simply dropped.
2) Local key update and node mobility lead to trust lost between one and its neighbors. Before neighboring nodes establish shared local keys, no traffic can be passed between them, which results in transmission delay in APPRP;
3) Route repair in AODV is not applicable in the protocol for the sake of privacy protection, as route repair requires identity information about the destination;
4) In AODV or MASK, intermediate nodes can reply to a route request if they know a route to the requested destination, while APPRP cannot do this as any intermediate node is not supposed to know either the source node or the destination node. Fig 3 Show that packet delivery ratio of SAPPRP. We can also see that AODV has the least delivery latency and MASK is between AODV and APPRP, but the packet delivery latency difference between APPRP and MASK is less than 100ms. Under the light traffic load APPRP's latency increases from 50ms to 90ms when node speed increases from 0m/s to10m/s. Under the heavy traffic load, APPRP's latency increases from about 100ms to more than 400ms for node speed from 0m/s to 10m/s.
Fig 3. Shows the packet delivery ratio of SAPPRP. In AODV, only three types of routing control packets, namely routing request packet, routing reply packet, and routing error packet. Before neighbouring nodes establish shared local keys, no traffic can be passed between them, which results in transmission delay in APPRP.The APPRP high throughput has compared to other Privacy routing protocols.

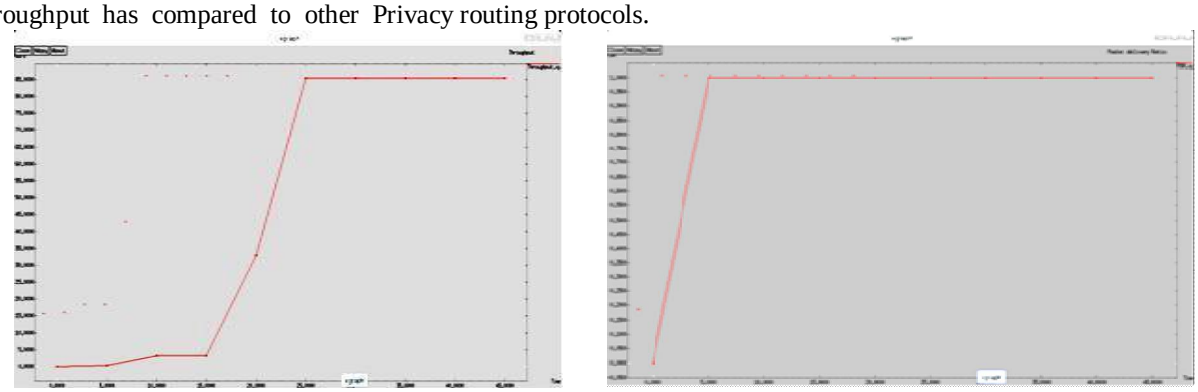

Fig.3. Throughput of APPRP and Packet delivery ratio of APPRP

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed an unobservable routing protocol APPRP based on group signature and ID-based cryptosystem for ad hoc networks. The design of APPRP offers strong privacy protection—completes unlinkability and content unobservability—for ad hoc networks. The security analysis demonstrates that APPRP not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. We implemented the protocol on ns2 and examined performance of APPRP, which shows that APPRP has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes. Future work along this direction is to study how to

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

defend against wormhole attacks, which cannot be prevented with APPRP. Also how to make the unobservable routing scheme resistant against DoS attacks is a challenging task that demands in-depth investigation.

REFERENCES

1. D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous Networks," in *Proc. IEEE WCNC'09*, Apr. 2009.
2. C. Perkins, E. Belding-Royer, S. Das, *et al.*, "RFC 3561 - Ad hoc On- Demand Distance Vector (AODV) Routing," *Internet RFCs*, 2003.
3. C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99), pp. 90–100, New Orleans, La, USA, February 1999.
4. D. B. Johnson, "Routing in ad hoc networks of mobile hosts," in Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, pp. 158–163, December 1994.
5. A. Back, U. Möller, and A. Stiglic, "Traffic analysis attacks and trade-offs in anonymity providing systems," in Proceedings of the 4th International Workshop on Information Hiding, pp. 245–257, Springer, 2001.
6. C. I. Fan, P. H. Ho, and R. H. Hsu, "Provably secure nested one-time secret mechanisms for fast mutual authentication and key exchange in mobile communications," IEEE/ACM Transactions on Networking, vol. 18, no. 3, pp. 996–1009, 2010.
7. D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," *Internet RFCs*, 2007.
8. J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in *Proc. ACM MobiHoc'03*, Jun. 2003, pp. 291–302.
9. J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. on Mobile Computing*, vol. 6, no. 8, pp. 888– 902, Aug. 2007.
10. A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks," in *Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04)*, Nov. 2004, pp. 618–624.
11. R. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks," in *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'05)*, Nov. 2005.
12. Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proc. IEEE INFOCOM 2005*, vol. 3, Mar. 2005, pp. 1940–1951.
13. Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On- Demand Routing in Mobile Ad hoc Networks," *IEEE Trans. on Wireless Comms.*, vol. 5, no. 9, pp. 2376–2386, Sept. 2006.
14. L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in *Proc. Int. Conf. On SECURECOMM'06*, Aug. 2006.
15. J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated Ad hoc Routing protocol," in *Proc. International Conf. on Information Security and Assurance (ISA'08)*, Apr. 2008.
16. S. William and W. Stallings, *Cryptography and Network Security, 4th Edition*. Pearson Education India, 2006